SEALED

ORIGINAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

UNITED STATES OF AMERICA

v.

KOLADE AKINWALE OJELADE (01)

No. 4:23-CR-043-O
[Supersedes Indictment Returned on February 15, 2023]

SUPERSEDING INDICTMENT

The Grand Jury Charges:

At all times material to this superseding indictment:

Introduction and Definitions

1. The term "phishing" refers to the practice of tricking internet users into revealing personal or confidential information—such as passwords—or allowing unauthorized access to computer systems or accounts. Phishing attacks sometimes use spam email messages or illegitimate websites designed to look like legitimate emails or websites.

2. A "forwarding rule" is a pre-programmed instruction that a person can set up in an email account to automatically send emails to another email account, without any additional user interaction. As used here, the technique allowed an unauthorized user to intercept and view emails intended for another recipient by secretly sending a copy of emails to the unauthorized user, without alerting the intended recipient that the email was automatically forwarded.

3. The term "spoofing" refers to the practice of impersonating a party to an email communication. For example, when "John Doe" sends an email from "john.doe@gmail.com," the recipient of the email may only see "John Doe" displayed as the sender. A person pretending to be John Doe might create an email address of john.doe2@gmail.com and set the display name to "John Doe." If the recipient of the email does not look for the actual email address of the sender, the recipient may be tricked into believing the email came from the real John Doe.

4. The term "man-in-the-middle" attack refers to a technique where cyber attackers insert themselves into the flow of communications between two or more parties, often by spoofing. This enables the attacker to select which communications are delivered to the intended recipient, allowing the attacker to modify communications before they are delivered to the intended recipient.

5. The term "business email compromise" or "BEC" is a scheme through which criminals gain unauthorized access to a business's email account(s)—often through phishing—and then use that access to engage in various fraudulent schemes.

6. The following were companies engaged in real estate title transactions:

a. Title Company-1 was a title company with its principal place of business in Dallas, Texas.

b. Title Company-2 was a title company with its principal place of business in Colleyville, Texas.

c. Title Company-3 was a title company with its principal place of business in Ogallala, Nebraska.

d. Title Company-4 was a title company with its principal place of business in Colleyville, Texas.

e. Title Company-5 was a title company with its principal place of business in DeSoto, Texas.

f. Title Company-6 was a title company with its principal place of business in Southlake, Texas.

g. Title Company-7 was a title company with its principal place of business in Garland, Texas.

7. The following were individuals involved in the purchase and sale of real estate:

a. Real Estate Client-1 was a home buyer who resided in Birmingham, Alabama.

b. Real Estate Client-2 was a home buyer who resided in Lake Worth, Texas.

c. Real Estate Client-3 was a home buyer who resided in Fort Worth, Texas.

d. Real Estate Client-4 was a home seller who resided in Hurst, Texas.

e. Real Estate Client-5 was a home buyer who resided in Dallas, Texas.

f. Real Estate Client-6 was a home seller who resided in Irving, Texas.

g. Real Estate Client-7 was a home buyer who resided in Garland, Texas.

h. Real Estate Client-8 was a home buyer who resided in Greenwood Village, Colorado.

8. The following were real estate companies involved in the transaction of real estate:

a. Real Estate Company-1 was a real estate company with its principal place of business in Birmingham, Alabama.

b. Real Estate Company-2 was a real estate company with its principal place of business in North Richland Hills, Texas.

c. Real Estate Company-3 was a real estate company with its principal place of business in Fort Worth, Texas.

d. Real Estate Company-4 was a real estate company with its principal place of business in Arlington, Texas.

9. Each of the following entities was a financial institution within the meaning of 18 U.S.C. § 20:

a. Financial Institution-1 was a bank headquartered in San Antonio, Texas.

b. Financial Institution-2 was a bank headquartered in San Francisco, California.

c. Financial Institution-3 was a bank headquartered in McKinney, Texas.

d. Financial Institution-4 was a bank headquartered in New York, New York.

e. Financial Institution-5 was a mortgage lender headquartered in Dallas, Texas.

Defendant and Email Accounts Controlled by Defendant and his Coconspirators

10. The defendant, **Kolade Akinwale Ojelade**, is a Nigerian citizen and computer security expert who used his technical skills to engage in a business email compromise fraud scheme.

11. **Ojelade** and his coconspirators used email addresses such as batebuild@gmail.com, gregthatcher46@gmail.com, dgoenzalez@gmail.com, richyjames051@gmail.com, robinsechrist002@gmail.com, and others primarily as "Collection Accounts" to illegally intercept businesses' emails. **Ojelade** and his coconspirators would monitor these Collection Accounts to see when a potential large transaction was about to occur.

For example, **Ojelade** and his coconspirators used Collection Accounts to illegally intercept and monitor emails involving real estate-related documents like closing disclosures and wiring instructions.

12. **Ojelade** and his coconspirators used email addresses such as admin@harrietdeck.com, info.files1@comcast.net, info.files1@xfinity.com, office.fld@comcast.net, and others primarily as "Spoofing Accounts" to trick unwary businesses into believing they were emailing with legitimate counterparties when, in fact, they were emailing with **Ojelade** and his coconspirators. For example, **Ojelade** and his coconspirators would use these Spoofing Accounts to send fraudulent wiring instructions to a party involved in a real estate transaction.

13. **Ojelade** and his coconspirators used donkayandkevin@gmail.com, donkay47@gmail.com, and others primarily as "Management Accounts" to coordinate the overall operation of the fraud scheme, including phishing activities, selecting targets of opportunity, and coordinating between the Collection Accounts and Spoofing Accounts.

14. **Ojelade** also used email accounts such as donkay46@gmail.com, donkay46@icloud.com, koladoj@live.com, koladoj@outlook.com, and others for a variety of purposes.

Count One
Conspiracy to Commit Wire Fraud
(Violation of 18 U.S.C. § 1349 (18 U.S.C. § 1343))

15. Paragraphs 1 through 14 of this superseding indictment are incorporated.

16. From in or about November 2013 through in or about March 2023, in the Northern District of Texas and elsewhere, the defendant, **Kolade Akinwale Ojelade**, along with others known and unknown, did knowingly and willfully combine, conspire, confederate, and agree to violate 18 U.S.C. § 1343, that is, to knowingly execute a scheme and artifice to defraud companies, individuals, schools, government entities, and others, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice caused to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, including emails, wiring instructions, bank wires, and faxes.

Object of the Conspiracy

17. It was the object of the conspiracy for **Ojelade** and his coconspirators to unlawfully enrich themselves and others by fraudulently causing victims—namely, companies, individuals, schools, government entities, and others—to transfer money to bank accounts held by **Ojelade** and his coconspirators.

Manner and Means of the Conspiracy and Scheme to Defraud

18. **Ojelade** and his coconspirators used the following manners and means, among others, to accomplish the object of the conspiracy and the scheme to defraud:

a. **Ojelade** and his coconspirators would send phishing emails to targeted victims to compromise victims' email accounts and provide **Ojelade** and his coconspirators with unauthorized access to those accounts. The primary targets of **Ojelade** and his coconspirators in this scheme were businesses related to real estate, which were often engaged in large lump-sum wire transactions.

b. **Ojelade** and his coconspirators would then access the compromised accounts and create forwarding rules and other means by which he and his coconspirators would use Collection Accounts to illegally intercept and view the targeted victims' emails.

c. **Ojelade** and his coconspirators would monitor the victims' emails to determine when a large wire transaction was about to take place. At that point, **Ojelade** and his coconspirators would use Spoofing Accounts to insert themselves into the conversation by spoofing—or pretending to be—the other parties.

d. **Ojelade** and his coconspirators then used this spoofing technique to intercept, modify, and retransmit wire payment instructions sent by one party to the other. That is, unbeknownst to the victims, **Ojelade** and his coconspirators changed the wiring instructions so that, instead of a victim sending money to an account controlled by a legitimate counterparty, the victim sent money to an account controlled by **Ojelade** and his coconspirators.

e. Once the money was wired into **Ojelade's** and his coconspirators' bank accounts, **Ojelade** and his coconspirators withdrew the money or otherwise transferred it into other accounts that they controlled.

Overt Acts

19. In furtherance of the conspiracy and to effect its object, in the Fort Worth Division of the Northern District of Texas and elsewhere, **Ojelade** and his coconspirators committed the following overt acts, among others:

a. On or about September 6, 2017, **Ojelade** and his coconspirators conducted a man-in-the-middle attack, in which they spoofed counterparties to a real estate transaction involving Real Estate Client-1 and Real Estate Company-1. That is, when Real Estate Client-1 thought he was communicating with Real Estate Company-1, he was in fact communicating with **Ojelade** and his coconspirators, who used the email address info.files1@comcast.net to carry out the attack.

b. On or about September 6, 2017, Real Estate Client-1 attempted to wire the down payment for a new home to Real Estate Company-1. However, **Ojelade** and his coconspirators had changed the routing instructions so that Real Estate Client-1 instead sent the money to **Ojelade** and his coconspirators. As a result, Real Estate Client-1 lost his down payment.

c. As described in Count 2, on or about September 11, 2017, in the Northern District of Texas and elsewhere, **Ojelade** and his coconspirators conducted a man-in-the-middle attack, in which they repeatedly spoofed counterparties to a real estate transaction involving Real Estate Client-2 and Title Company-1. That is, when Real Estate Client-2 and Title Company-1 thought they were communicating with each other, they were, in fact, both communicating with **Ojelade** and his coconspirators, who were using the email address info.files1@comcast.net to misrepresent themselves to be the two parties.

d. On or about September 11, 2017, in the Northern District of Texas and elsewhere, Real Estate Client-2 attempted to wire the down payment for a new home to Title Company-1. However, **Ojelade** and his coconspirators had changed the routing instructions so that Real Estate Client-2 instead sent the money from his account at Financial Institution-1 to **Ojelade** and his coconspirators at an account at Financial Institution-2, rather than Title Company-1's bank, Financial Institution-3. As a result, Real Estate Client-2 lost his down payment and was unable to purchase the home.

e. As described in Count 3, on or about February 23, 2018, in the Northern District of Texas and elsewhere, **Ojelade** and his coconspirators used the email address gregthatcher46@gmail.com to intercept an email from Title Company-2 to Real Estate Company-2. That same day, gregthatcher46@gmail.com forwarded the intercepted email to donkay47@gmail.com and copied info.files1@comcast.net.

On or about the same day, donkay47@gmail.com forwarded the email to info.office1@comcast.net. The email pertained to a real estate transaction.

f. From or about October 2020 to November 2020, **Ojelade** and his coconspirators used an unauthorized forwarding rule on an email account belonging to Title Company-3 that automatically forwarded emails to the Collection Account bate.build@gmail.com. During the same time period, bate.build@gmail.com forwarded emails collected from Title Company-3 to donkay47@gmail.com. The forwarded messages pertained to multiple real estate transactions being handled by Title Company-3.

g. On or about November 3, 2020, **Ojelade** and his coconspirators spoofed emails to misrepresent themselves to be Title Company-3 in order to trick Real Estate Client-8 into sending funds via wire to a bank account at Financial Institution-4 controlled by **Ojelade** and his coconspirators.

20. Also in furtherance of the conspiracy and to effect its object, in the Northern District of Texas and elsewhere, **Ojelade** and his coconspirators committed the acts described in Counts Two through Twelve.

Count Two
Wire Fraud Affecting a Financial Institution
(Violation 18 U.S.C. §§ 1343 and 2)

21. Paragraphs 1 through 20 of this superseding indictment are incorporated.

22. On or about the September 11, 2017, in the Fort Worth Division of the Northern District of Texas and elsewhere, defendant **Kolade Akinwale Ojelade**, along with others known and unknown, aiding and abetting each other, knowingly devised and intended to devise the scheme to defraud described in Count One, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme, transmitted and caused to be transmitted by means of wire communications in interstate and foreign commerce, writings, signals, pictures, and sounds, namely, an email sent from outside the state of Texas to Real Estate Client-2 in the Northern District of Texas from a spoofed account using the email address info.files1@comcast.net and purporting to be Title Company-1 and containing fraudulent instructions for sending money to a coconspirators' bank account ending in 2155 at Financial Institution-2, and in doing so affected a financial institution, namely, Financial Institution-1 and Financial Institution-2.

All in violation of 18 U.S.C. §§ 1343 and 2.

Counts Three – Seven
Wire Fraud
(Violation 18 U.S.C. §§ 1343 and 2)

23. Paragraphs 1 through 20 of this superseding indictment are incorporated.

24. On or about the dates set forth below, in the Fort Worth Division of the Northern District of Texas and elsewhere, defendant **Kolade Akinwale Ojelade**, along with others known and unknown, aiding and abetting each other, knowingly devised and intended to devise the scheme to defraud described in Count One, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises as described in Count One, and for the purpose of executing such scheme, caused to be transmitted the interstate and foreign wire communications listed below, each constituting a separate count:

Count	Date	Description of Wire
3	2/23/2018	Email sent from Title Company-2, in the Northern District of Texas, to Real Estate Company-2 about a property in Fort Worth, Texas, intercepted by gregthatcher46@gmail.com and routed through servers outside the state of Texas
4	9/19/2018	Email sent from Title Company-4, in the Northern District of Texas, to Real Estate Company-3, Real Estate Client-4, and others about a property in Fort Worth, Texas, intercepted by robinsechrist002@gmail.com and routed through servers outside the state of Texas
5	9/25/2018	Email from spoofed account using office.fld@comcast.net, sent from and routed through servers outside the state of Texas, into the Northern District of Texas, purporting to be from Title Company-5 to Real Estate Company-4, about a property in DeSoto, Texas

6	10/14/2019	Email sent from Title Company-6, in the Northern District of Texas, to Real Estate Company-3 and Real Estate Client-6 about a property in Dallas, Texas, intercepted by robinsechrist002@gmail.com and routed through servers outside the state of Texas
7	1/15/2021	Email sent from Title Company-7, in the Northern District of Texas, to Financial Institution-5 about property in Garland, Texas, intercepted by donkay47@gmail.com and routed through servers outside the state of Texas

All in violation of 18 U.S.C. §§ 1343 and 2.

Counts Eight Through Twelve
Aggravated Identity Theft
(Violation of 18 U.S.C. §§ 1028A and 2)

25. Paragraphs 1 through 20, and paragraph 24 of this superseding indictment are incorporated.

26. On or about the dates set forth in the table below, in the Fort Worth Division of the Northern District of Texas and elsewhere, defendant **Kolade Akinwale Ojelade**, along with others known and unknown, aiding and abetting each other, did knowingly transfer, possess, and use, without lawful authority, the means of identification of another person, that is, the names and addresses of the victims identified in the table below, during and in relation to felonies enumerated in 18 U.S.C. § 1028A, that is, wire fraud and conspiracy to commit wire fraud, in violation of 18 U.S.C. §§ 1343 and 1349, as described in the counts referenced in the table below, knowing that the means of identification belonged to another actual person:

Count	Date	Victim	Related to Counts
8	2/23/2018	Real Estate Client-3	Counts One and Three
9	9/19/2018	Real Estate Client-4	Counts One and Four
10	9/25/2018	Real Estate Client-5	Counts One and Five
11	10/14/2019	Real Estate Client-6	Counts One and Six
12	1/15/2021	Real Estate Client-7	Counts One and Seven

All done in violation of 18 U.S.C. §§ 1028A(1) and 2.

Forfeiture Notice
(18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c); 18 U.S.C. § 982(a)(2)(A))

27. Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), upon conviction for any violation of 18 U.S.C. §§ 1343 and/or 1349, the defendant, **Kolade Akinwale Ojelade**, shall forfeit to the United States of America any property, real or personal, constituting or derived from proceeds traceable to the respective offense, as well as the underlying scheme to defraud and/or conspiracy.

28. Pursuant to 18 U.S.C. § 982(a)(2)(A), upon conviction for any violation of 18 U.S.C. § 1343 affecting a financial institution, the defendant, **Kolade Akinwale Ojelade**, shall forfeit to the United States of America any property, real or personal, constituting, or derived from proceeds obtained directly or indirectly, as the result of the offense, as well as the underlying scheme to defraud.

29. The property subject to forfeiture may include a "money judgment" against the defendant for the total amount of proceeds traceable to and/or obtained from the respective offense(s) of conviction, as well as the underlying scheme to defraud and/or conspiracy.

30. The government may seek the forfeiture of substitute property from the defendant, as allowed by 21 U.S.C. § 853(p) and as applicable under 28 U.S.C. § 2461(c).

A TRUE BILL.

FOREPERSON

LEIGHA SIMONTON
UNITED STATES ATTORNEY

MATTHEW WEYBRECHT
Assistant United States Attorney
State Bar of Texas No. 24102642
Telephone: 817-252-5200
Fax: 817-252-5455
Email: matthew.weybrecht@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THE UNITED STATES OF AMERICA

v.

KOLADE AKINWALE OJELADE (01)

SUPERSEDING INDICTMENT

18 U.S.C. § 1349 (18 U.S.C. § 1343)
Conspiracy to Commit Wire Fraud
Count 1

18 U.S.C. §§ 1343 and 2
Wire Fraud Affecting a Financial Institution
Count 2

18 U.S.C. §§ 1343 and 2
Wire Fraud
Counts 3 – 7

18 U.S.C. §§ 1028A and 2
Aggravated Identity Theft
Counts 8 – 12

8 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c); 18 U.S.C. § 982(a)(2)(A)
Forfeiture Notice

A true bill rendered

FORT WORTH FOREPERSON
Filed in open court this 10th day of May, 2023.

Warrant to be Issued

Hal R. Ray, Jr.
UNITED STATES MAGISTRATE JUDGE
District Court Number: 4:23-CR-043-O